Groups and Graphs
Lecture III: growths

Vietri, 6-10 giugno 2016

Let $\Gamma = (V, E)$ be a k-regular graph, and fix a vertex, 'the origin', and call it 1.

For every $i \in \mathbb{N}$ we like to describe the distribution $\nu_i : V \to [0, 1]$, where for every $x \in V$, $\nu_i(x)$ is the probability that a random walk of length i starting at 1 ends in x (here, for a random walk it is intended that at every vertex the walk takes the next edge with equal probability $1/k$).

So, ν_0 takes value 1 in the origin and 0 in all other vertices, while $\nu_1(x) = 1/k$ if x is adjacent to 1, otherwise $\nu_1(x) = 0$. Thus, if $A = A(\Gamma)$, then $\nu_1 = \frac{1}{k} A\nu_0$.
In general,

$$\nu_{i+1} = \frac{1}{k} A\nu_n = \frac{1}{k^{n+1}} A^{n+1}\nu_0.$$

In particular, for every $i \geq 1$

$$\nu_i(1) = \frac{A^i_{1,1}}{k^i} = \frac{\omega_i}{k^i}$$

where $\omega_i = A^i_{1,1}$ is the number of distinct closed walks of length i at the origin.

Write $\hat{A} = \frac{1}{k}A$, then for every $i \geq 0$, $\nu_{i+1} = \hat{A}\nu_i$.

Let $|V| = n$ and let $\mathbf{u}$ be the uniform probability distribution on V: i.e.

$$\mathbf{u}(x) = 1/n \text{ for every } x \in V.$$

Let $i \geq 1$; since ν_i and $\mathbf{u}$ are probability measures, their difference $\nu_i - \mathbf{u}$ is a zero-sum function on V, that is $\nu_i - \mathbf{u} \in \mathcal{Z}^{\perp}$. Observe that, being $\mathbf{u}$ a constant, $\hat{A}\mathbf{u} = \mathbf{u}$. Therefore

$$\langle \nu_{i+1} - \mathbf{u}, \nu_{i+1} - \mathbf{u} \rangle = \langle \hat{A}(\nu_i - \mathbf{u}), \hat{A}(\nu_i - \mathbf{u}) \rangle = \langle \hat{A}^2(\nu_i - \mathbf{u}), \nu_i - \mathbf{u} \rangle.$$

Now, if μ is the largest absolute value of an eigenvalue $\neq k$ of A, then

$$||\nu_{i+1} - \mathbf{u}||^2 = \langle \hat{A}^2(\nu_i - \mathbf{u}), \nu_i - \mathbf{u} \rangle \leq \mu^2/k^2 ||\nu_i - \mathbf{u}||^2$$

That is $||\nu_{i+1} - \mathbf{u}|| \leq (\mu/k)||\nu_i - \mathbf{u}||$; and, by an easy induction

$$||\nu_i - \mathbf{u}|| \leq \left(\frac{\mu}{k}\right)^i \sqrt{\frac{n-1}{n}}$$

- *The smaller is μ, the faster $\{\nu_i\}_{i \geq 1}$ converges to the uniform distribution.*

Now, let $\Gamma = \Gamma[G, S]$ be a Cayley graph, for S a symmetrical subset of G, $|S| = k$. Then, observe that for every $i \in \mathbb{N}$ and $x \in G$, $\nu_i(x)$ is the probability that a word of length i in S represents the element x in G; moreover ν_i is symmetrical, in the sense that $\nu_i(x) = \nu_i(x^{-1})$ for every $x \in G$

In the space $\mathcal{C}(\Gamma)$ a *convolution product* $*$ is defined by setting

$$(f * g)(x) = \sum_{y \in G} f(xy^{-1})g(y).$$

For $f \in \mathcal{C}(\Gamma)$ and $m \geq 1$, write $f^{(m)} = f * \cdots * f$ (m times). It is easy to verify that if f is a symmetrical probability measure, then also $f^{(m)}$ is a symmetrical probability measure. Also, it is easy to check that, for every $i \geq 1$,

$$\nu_i = \nu_1^{(i)}.$$

GROWTH.

Let G be a finitely generated group, A a finite set of symmetric generators. A distance in G is defiined by $d_A(g,h) = \ell_A(g^{-1}h)$. For $r \geq 0$

$$B(1,r) = \{g \in G \mid \ell_A(g) \leq r\} = (A \cup \{1\})^r$$

the growth function (for A in G) is the integer-valued function

$$r \to |B(1,r)|.$$

In infinite (finitely generated) groups this concept originated a rich and deep theory (e.g. the celebrated Gromov's Theorem).

For finite groups, interest is much more recent, but resulted already in important achievements. While in infinite groups, A is small (finite) and one is interested the behaviour for large r, in the finite case, roughly speaking, one is interested in 'some' initial steps of the growth, and when A is relatively large.

example. In $\mathbb{Q}$ consider an arithmetic progression

$$A = \{\pm a, \pm 2a, \ldots, \pm ka\}$$

Additively (i.e. as a subset of $(\mathbb{Q}, +)$), A grows "slowly," in fact $|A + A| \leq 2|A|$ while multiplicatively (as a subset of $(\mathbb{Q}^*, \cdot)$) it grows "fast", for $|A^2| \sim |A|^2$.

example. In $\mathbb{Q}$ consider an arithmetic progression

$$A = \{\pm a, \pm 2a, \ldots, \pm ka\}$$

Additively (i.e. as a subset of $(\mathbb{Q}, +)$), A grows "slowly," in fact $|A + A| \leq 2|A|$ while multiplicatively (as a subset of $(\mathbb{Q}^*, \cdot)$) it grows "fast", for $|A^2| \sim |A|^2$.

example 2. A consequence of Freiman Theorem (which describes all finite subset of $\mathbb{Z}$ that grow slowly).

Let A be a finite subset of $\mathbb{Z}$ such that $|A + A| \leq 3|A| - 3$. Then A is contained in an arithmetic progression of length at most $2|A| + 2$

In abelian groups, a result of Ruzsa ensures that if $|AA|$ is 'small' (when compared to $|A|$), then $|A^3|$ is small compared to A^2, and so on
(in a sense: A^2 sets the pace).

In abelian groups, a result of Ruzsa ensures that if $|AA|$ is 'small' (when compared to $|A|$), then $|A^3|$ is small compared to A^2, and so on
(in a sense: A^2 sets the pace).

example. Suppose G is not abelian, let H be a proper subgroup of G, $g \in G - N$, and $A = \{g\} \cup H$. Then $A^2 = \{g^2\} \cup gH \cup Hg \cup H$, hence $|A^2| \leq 3|A|$. While A^3 contains the double coset HgH which may be very large.

In abelian groups, a result of Ruzsa ensures that if $|AA|$ is 'small' (when compared to $|A|$), then $|A^3|$ is small compared to A^2, and so on
(in a sense: A^2 sets the pace).

example. Suppose G is not abelian, let H be a proper subgroup of G, $g \in G - N$, and $A = \{g\} \cup H$. Then $A^2 = \{g^2\} \cup gH \cup Hg \cup H$, hence $|A^2| \leq 3|A|$. While A^3 contains the double coset HgH which may be very large.

For arbitrary groups, it is the third power A^3 that sets the pace. Better: if A^3 is small with respect A, then all further powers are small (with respect the previous one)

Lemma (Ruzsa triangle inequality)

Let A, B, C finite subsets of the group G. Then

$$|AC^{-1}||B| \leq |AB^{-1}||BC^{-1}|.$$

Corollary

Let $A = A^{-1}$ be a subset of the group G. Then, for every $k \geq 3$

$$\frac{|A^k|}{|A|} \leq \left(\frac{|A^3|}{|A|}\right)^{k-2}$$

The concept of approximate subgroup (i.e.'slowly growing subset') is fundamental

Let G be a group, $K \geq 1$ and $A \subset G$. A is a K-approximate subgroup if

- $1 \in A = A^{-1}$;
- there exists a symmetric $X \subseteq G$ with $|X| \leq K$ such that $AA \subseteq XA$.

a K-approximate subgroup A is a slowly growing set: $|A^3| \leq K^2|A|$. Conversely

if A is symmetric, contains 1 and $|A^3| \leq K|A|$, then the set A^3 is a $K^{O(1)}$-approximate subgroup (this was shown by T. Tao). More:

Lemma (T. Tao)

There exists $C \geq 1$ such that if A is a finite subset of a group G, with $|A^2| \leq K|A|$, for $K \geq 1$, then A is contained in the union of at most K^C cosets of a K^C-approximate subgroup H of size $|H| \leq K^C|A|$.

Here is one of the most useful results in the so-called 'additive combinatorics". We will not have time to discuss it into any detail.

Theorem (Balog-Szemerédi-Gowers-Tao)

Let A, B be finite subsets of the group G. Suppose that

$$E(A,B) \geq |A|^{3/2}|B|^{3/2}/K.$$

Then there exist $A' \subset A$, $B' \subset B$ such that $|A|/K << |A'|$, $|B|/K << |B'|$ and $|A'B'| << K\sqrt[8]{|A||B|}$

Here $E(A,B)$ is the *multiplicative energy*

$$E(A,B) = \left|\{(a_1,a_2,b_1,b_2) \in A \times A \times B \times B \ \mid \ a_1b_1 = a_2b_2\}\right| = ||1_A * 1_B||^2$$

(1_A and 1_B) are, respectively, the characteristic function of A and of B.)

Lemma (flattening)

There exists a constant $R > 0$ such that the following holds. Let $K \geq 2$, G a finite group, and ν a probability measure on G with $\nu(g) = \nu(g^{-1})$ for all $g \in G$; then

(i) *either $||\nu * \nu|| \leq K^{-1}||\nu||$, or*

(ii) *there is a K^R-approximate subgroup H of G, with*

$$K^{-R}/||\nu||^2 \leq |H| \leq K^R/||\nu||^2$$

and an element $x \in G$ such that $\nu(xH) \geq K^{-R}$.

Just to give an idea, we treat the simplest case in which ν is the probability measure centered in a symmetric subset A, i.e.

$$\nu = 1_A/|A|$$

where 1_A is the characteristic function of $A = A^{-1} \subseteq G$.

Then

$$||\nu||^2 = \sum_{x \in A} |A|^{-2} = |A|^{-1}, \quad ||\nu * \nu||^2 = |A|^{-4}||1_A * 1_A||^2 = |A|^{-4}E(A,A).$$

Suppose (i) does not occur; that is $||\nu * \nu|| \geq K^{-1}||\nu||$. Then

$$|A|^{-4}E(A,A) \geq K^{-2}|A|^{-1}$$

that is

$$E(A,A) \geq K^{-2}|A|^{3/2}|A|^{3/2}$$

Then

$$||\nu||^2 = \sum_{x \in A} |A|^{-2} = |A|^{-1}, \quad ||\nu * \nu||^2 = |A|^{-4}||1_A * 1_A||^2 = |A|^{-4}E(A,A).$$

Suppose (i) does not occur; that is $||\nu * \nu|| \geq K^{-1}||\nu||$. Then

$$|A|^{-4}E(A,A) \geq K^{-2}|A|^{-1}$$

that is

$$E(A,A) \geq K^{-2}|A|^{3/2}|A|^{3/2}$$

We may apply Balog et al. Theorem: there exist $A_1, A_2 \subseteq A$ with $|A_i| >> K^{-2}|A|$ and

$$|A_1 A_2| << K^2 \sqrt[8]{|A_1||A_2|}$$

By Ruzsa triangle inequality, if $|A_1| \geq |A_2|$,

$$|A_1 A_1| \leq |A_2|^{-1} |A_1 A_2|^2 \leq |A_1 A_2|^4 \leq K^8 |A_1|$$

(for semplicity, we are ignoring the multiplicative constants)

By Ruzsa triangle inequality, if $|A_1| \geq |A_2|$,

$$|A_1 A_1| \leq |A_2|^{-1} |A_1 A_2|^2 \leq |A_1 A_2|^4 \leq K^8 |A_1|$$

(for semplicity, we are ignoring the multiplicative constants)

By Tao's Lemma, there is a K^R-approximate subgroup H, with $|H| \leq K^R |A_1|$, such that A_1 is contained in at most K^R left translates xH. For at least one of these elements x

$$|xH \cap A_1| \geq K^{-R} |A_1|$$

As, in this case, $||\nu||^2 = |A|^{-1}$ we have that H is the approximate subgroup we looked for. In fact, since $A_1 \subseteq A$,

$$\nu(xH) \geq \nu(xH \cap A_1) = (|xH \cap A_1|)|A|^{-1} \geq K^{-R} |A_1|/|A| \geq K^{-(R+2)}$$

(replace R by $R+2$).

The seminal result for growth in finite groups, is the following Theorem, published in 2008.

Theorem (Helfgott)

There exists $\delta > 0$ such that, for every prime p and every generating set A of $G = SL(2, p)$, one has

- *either* $(A \cup A^{-1} \cup \{1\})^3 = G$, *or*
- $|A^3| \geq |A|^{1+\delta}$.

The original Helfgott's statement had, as first alternative, $A^k = G$, for some constant $1 \leq k \in \mathbb{N}$; it was soon realized that $k = 3$ would do in any case. At the end, we will mention some recent far-reaching extensions [Babai, Bourgain, Gamburd, Sarnak, Pyber, Szabò, Hrushovski, Dinai, Nikolov, Gill, Guralnik, Breuillard, Green, Tao: it is just the beginning of a much longer list]

Set

$$C = \frac{\log 3}{\log (1+\delta)}$$

Then, if A_p any symmetrical generating set of $G_p = SL(2,p)$, direct iterated application of Helfgott's Theorem yields

$$diam[\Gamma(G_p, A_p)] \leq (\log_{|A|}(|G_p|))^C$$

Hence, Babai/Seress conjecture (see Lecture I) is true for groups $SL(2,p)$.

If A is a generating subset of $SL(2,\mathbb{Z})$, $\bar{A} = A \cup A^{-1}$ and, for any prime p, $A_p = \pi_p(\bar{A})$, we may do even better.

w.l.o.g. we may assume that A is a free set of generators of a free subgroup of $SL(2,\mathbb{Z})$. (continues in the next slide).

Since entries of elements in $\bar{A}$ do not exceed in absolute value a certain positive integer, there exists c, depending only on A, such that if $m \leq \log_c(p/2)$, then two products, $a_1, \ldots, a_m$ and $a'_1, \ldots, a'_m$ of elements in $(\bar{A} \cup \{1\})$, are equal in $SL(2,p)$, if and only if they are equal in $SL(2,\mathbb{Z})$.

In other words, around vertex 1, up to distance m, the Cayley graph $\Gamma[SL(2,p), A_p]$ looks like a tree. Thus, for $m = [\log_c(p/2)]$,

$$|(A_p \cup \{1\})^m| \geq (2|A| - 1)^m \geq p^\kappa,$$

with $\kappa \geq 1$ depending only on c (hence on A).

Then apply Helfgott's Theorem t times, where $\kappa(1+\delta)^t \geq 3$ (this does not depend on p). Have

$$|(A_p \cup \{1\})^{m \cdot 3^t})| \geq p^{\kappa(1+\delta)^t} \geq p^3 \geq |SL(2,p)|$$

Therefore,

$$diam(\Gamma[SL(2,p), A_p]) \leq m \cdot 3^t = O(\log p).$$

What does Helfgott's Theorem have to do with expanders?

We have seen that, by a result of Lubotzy, the graphs $\Gamma[SL(2,p), S_p]$ form a family of expanders, when, for every prime $p \geq 3$, $S_p = \{\sigma, \sigma^{-1}, \tau, \tau^{-1}\}$, with

$$\tau = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \qquad \sigma = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}.$$

But what about if we consider (for $p > 3$) generators

$$\tau = \begin{pmatrix} 1 & 3 \\ 0 & 1 \end{pmatrix} \qquad \sigma = \begin{pmatrix} 1 & 0 \\ 3 & 1 \end{pmatrix} \quad ?$$

Fore $A \subseteq SL(2,\mathbb{Z})$, and p a prime, denote by $A_p = \pi_p(A)$ the reduction of A modulo p and write $\bar{A}_p = (A_p \cup A_p^{-1}) - \{1\}$

Theorem (Bourgain, Gamburd)

Let $A \subseteq G = SL(2,\mathbb{Z})$, and suppose that A_p generates $SL(2,p)$ for sufficiently large p. Then there exists C such that the family

$$\Gamma[SL(2,p), \bar{A}_p] \quad (p \geq C)$$

is a family of expanders.

Write $G = SL(2, \mathbb{Z})$ and, for every prime p, π_p for the reduction modulo p. Suppose (for simplicity) that $A \subseteq G$ is the free generating set of a free subgroup of G (thus, if $|A| = k$, then its symmetrized $\bar{A} = A \cup A^{-1}$ contains $2k$ elements). For any prime p, let $A_p = \pi_p(\bar{A})$. For a sufficiently large p, $|A_p| = 2k$.

Let $\Gamma = \Gamma[SL(2, p), A_p]$. Consider the symmetric probability measure $\nu = \nu_1 \in \mathcal{C}(\Gamma)$ defined by, for $x \in SL(2, p)$,

$$\nu(x) = \begin{cases} \frac{1}{2k} \text{ if } x \in A_p \\ 0 \text{ if } x \notin A_p \end{cases}$$

By the remarks at the beginning of this lecture, for every $\ell \geq 1$,

$$\nu^{(\ell)}(1) = \nu_\ell(1) = \frac{A_{1,1}^\ell}{(2k)^\ell} = \frac{\omega_\ell}{(2k)^\ell}$$

We then have, for $\ell \geq 1$ (writing $SL(2,p) = G_p$),

$$||\nu^{(\ell)}||^2 = \sum_{x \in G_p} (\nu^{(\ell)}(x))^2 = \sum_{x \in G_p} \nu^{(\ell)}(x^{-1})\nu^{(\ell)}(x) = \nu^{(2\ell)}(1) = \frac{\omega_{2\ell}}{(2k)^{2\ell}}$$

(where $||\nu^{(\ell)}||^2 =< \nu^{(\ell)}, \nu^{(\ell)} >$)

Observe further that if $n = |SL(2,p)|$ then

$$n\omega_{2\ell} = tr(A^{2\ell}) = \sum_{i=0}^{n=1} \mu_i^{2\ell} > m_1 \mu_1^{2\ell}$$

where m_1 is the multiplicity of the eigenvalue μ_1 of A.

Now, all non-trivial irreducible $\mathbb{C}$-representation of $SL(2,p)$ have dimension

$$d \geq \frac{p-1}{2},$$

and so (lecture 3)

every eigenvalue $\mu_i \neq \mu_0 = 2k$ of the matrix A has multiplicity $\geq \frac{p-1}{2}$.

Remembering that $n = |SL(2,p)| = p(p^2-1)$, we obtain

$$\frac{p-1}{2}\mu_1^{2\ell} < p(p^2-1)\omega_{2\ell} = p(p^2-1)(2k)^{2\ell}||\nu^\ell||^2$$

hence

$$\mu_1^{2\ell} < 2p(p+1)(2k)^{2\ell}||\nu^\ell||^2. \tag{1}$$

Now, suppose we have the following

Lemma (BG)

For all $\bar{\delta} > 0$, there exists C such that, for $\ell \geq C \log_{2k} p$

$$||\nu^{(\ell)}|| < p^{-\frac{3}{2}+\bar{\delta}}. \tag{2}$$

Then, for $\ell \geq C \log_{2k} p$, from (1)

$$\mu_1^{2\ell} < 2p(p+1)(2k)^{2\ell} p^{-3+2\bar{\delta}} \leq 3(2k)^{2\ell} p^{-1+2\bar{\delta}}$$

so

$$\frac{\mu_1^{2\ell}}{(2k)^{2\ell}} < 3p^{-1+2\bar{\delta}} < 1$$

($2\bar{\delta}$ does not depend on p). Hence

$$2k - \mu_1 > \epsilon > 0$$

where ϵ depends only on A.

steps in the proof of Lemma (BG).

(1) *there exist constant C and $\eta > 0$ (depending only on A), such that, for a large enough p, and $m = [C \log p]$*

$$\nu^{(m)}(1) \leq p^{-\eta}.$$

this is obtained in a way similar, even if less strightforward, to the one we followed in the proof of the logarithmic bound for the diameter. There exists C, depending only on A, such that, if $p \geq C^m$, then around vertex 1, up to distance m, the Cayley graph $\Gamma[SL(2,p), A_p]$ is a tree.

Hence, the number ω_m of walks of length m, from 1 back to 1, in $\Gamma[SL(2,p), A_p]$ is the same as in the free group of rank k, that is the *number of words of length ℓ in $\bar{A}$, that reduce to identity*. From known facts:

$$\omega_m \leq C_0 p^{-\eta} \text{ for some } \eta > 0 \text{ depending only on } C \text{ (thus, on } A)$$

Then, just recall that

$$\omega_m = A^m_{1,1} = (2k)^m \nu^{(m)}(1).$$

(2) $\nu^{(m)}(H) \leq p^{-\eta}$ *for every* $H < G$. (here $G = SL(2,p)$)

this is not really difficult, and depends on the very well known fact that every proper subgroup of $SL(2,p)$ is metabelian.
(in the extensions to higher rank this point is much more delicate)

Observe that (2) implies, in particular, $\nu^{(m)}(g) \leq p^{-\eta}$ for every $g \in G$. Therefore (Young's inequality), for every $g \in G$,

$$(\nu * \nu)(g) = \sum_{x \in G} \nu(gx^{-1})\nu(x) \leq \sum_{x \in G} p^{-\eta}\nu(x) = p^{-\eta}$$

Consider $\nu = \nu^{(m)}, \nu^{(2m)}, \nu^{(4m)}, \ldots$

Then, by what observed above, for every $g \in G$

$$\nu(g) \leq p^{-\eta}$$

(3) *Suppose that, for some $\delta_1 > 0$ (which we are free to set, provided it is independent on p), if $K = p^{\delta_1}$, we have $||\nu * \nu|| \leq K^{-1}||\nu||$ for all such ν.*

Then at step $r = [\frac{3}{2}\delta_1^{-1}] + 1$, we have

$$||\nu^{(2^r m)}|| \leq p^{-\delta_1 r} \leq p^{-\frac{3}{2}}$$

and we are done.

(4) *With δ_1 as in point 3, suppose $||\nu * \nu|| > K^{-1}||\nu||$ for some ν.*

by Flattening Lemma there is a K^R-approximate subgroup H of G and $x \in G$ such that

$$|H| \leq K^R||\nu||^{-2} = p^{R\delta_1}||\nu||^{-2} \qquad \text{and} \qquad \nu(Hx) > K^{-R} = p^{-R\delta_1}.$$

(4.1) *Suppose that* $L = \langle H \rangle < G$.

Choose δ_1 such that $2R\delta_1 \leq \eta$. Then, if $\nu = \nu^{(2^\ell m)}$

$$\nu^{(2^{\ell+1} m)}(L) = \sum_{a \in L} \sum_{g \in G} \nu(ag)\nu(g) \geq \sum_{g \in Lx} \nu(g) \sum_{a \in L} \nu(ag) = \nu(Lx)^2 > p^{-\eta}$$

in contradiction with point (2)

$$\nu^{(m)}(L) \leq p^{-\eta}$$

[we have used the fact - exercise - that if ν is a symmetric probability measure, and $L \leq G$, then $\nu^{2\ell}(L) \geq \nu^{2(\ell+1)}(L)$, and assumed, as it is possible, m even]

(4.2) *H is a set of generators of G.* (Helfgott's case)

Since H is a K^R-approximate subgroup,

$$|H^3| \leq K^{2R}|H| \leq K^{3R}||\nu||^{-2} = p^{3R\delta_1}||\nu||^{-2}.$$

Now, Helfgott's Theorem implies that either $H^3 = G$ or $|H^3| \geq |H|^{1+\delta}$.

In the first case, $|G| \leq |H^3| \leq p^{3R\delta_1}||\nu||^{-2}$, and so

$$||\nu||^2 \leq p^{3R\delta_1}|G|^{-1} \leq \frac{p}{p-1}p^{3R\delta_1-3}.$$

For any δ_1 smaller or equal a value depending only on R, and large enough p, we obtain, for some $\ell = 2^r m$,

$$||\nu^{(\ell)}|| = ||\nu|| \leq p^{-\frac{3}{2}+\bar{\delta}}.$$

In the second case, from $|H|^{1+\delta} \leq |H^3| \leq p^{2R\delta_1}|H|$ we have

$$|Hx|^{\delta} = |H|^{\delta} \leq p^{2R\delta_1}$$

Therefore

$$p^{-R\delta_1\delta} < \nu(Hx)^{\delta} \leq |Hx|^{\delta} p^{-\eta\delta} \leq p^{2R\delta_1 - \eta\delta}$$

hence

$$\eta\delta \leq R\delta_1(2-\delta)$$

which is contradicted by a suitable choice of δ_1.

The following is due to Pyber and Szabò, and, in a slightly less general form, Breuillard, Green and Tao.

Theorem

Let L be a finite simple group of Lie type of rank r, and A a generating set of L. Then either $A^3 = L$ or

$$|A^3| > |A|^{1+\epsilon}$$

where $\epsilon > 0$ depends only on r.

A consequence is

Theorem

Let L be a finite simple group of Lie type of rank r, and A a symmetric generating set of L. Then

$$diam(\Gamma[L, A]) < (\log |L|)^{c(r)}$$

where $c(r)$ depends only on r.